Powiat Nowomiejski
ul. Rynek 1
13-300 Nowe Miasto Lubawskie

Zapytanie ofertowe

nr GM.272.2.1.2025, na:

przegląd, opracowanie i dostosowanie do nowych wymagań oraz wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, audyty i szkolenie z zakresu cyberbezpieczeństwa

o wartości nie przekraczającej wyrażonej w złotych równowartości kwoty określonej w art. 2 ust. 1 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tekst jednolity Dz.U. z 2024 poz. 1320).

Nowe Miasto Lubawskie, 26 lutego 2025 r.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

1. Nazwa i dane adresowe Zamawiającego

Zamawiający:	Powiat Nowomiejski
Adres:	ul. Rynek 1, 13-300 Nowe Miasto Lubawskie
Telefon:	+48 56 472 42 20
E-mail:	sekretariat@powiat-nowomiejski.pl zamowienia@powiat-nowomiejski.pl
ESP (ePUAP)	/spnml/ESP
Strona internetowa:	https://samorzad.gov.pl/web/powiat-nowomiejski
Strona BIP:	https://bip.powiat-nowomiejski.pl
NIP:	877-14-60-784
REGON:	871118879
Godziny urzędowania:	poniedziałek 7:15 – 15:15 wtorek 7:15 – 15:15 środa 7:15 – 15:15 czwartek 7:15 – 15:15 piątek 7:15 – 15:15
Zamawiający:	Powiat Nowomiejski

2. Wstęp

Zamówienie jest realizowane w ramach grantu w projekcie grantowym **„Cyberbezpieczny Samorząd”** współfinansowanym przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: *Zaawansowane usługi cyfrowe*, Działanie 2.2. – *Wzmocnienie krajowego systemu cyberbezpieczeństwa*, na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0922/ FERC.02.02-CS.01-001/23/2024 z dnia 25 kwietnia 2024 r. W ramach projektu przewidziano przegląd, opracowanie i dostosowanie do nowych wymagań oraz wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), audyt SZBI, audyt zgodności z wymaganiami Rozporządzenia KRI oraz przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry Starostwa Powiatowego w Nowym Mieście Lubawskim.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

3. Tryb udzielenia zamówienia

1. Na podstawie art. 2 ust. 1 pkt. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych niniejsze postępowanie nie podlega przepisom ww. ustawy.
2. Postępowanie przeprowadzone jest zgodnie z regulaminem udzielania zamówień publicznych o wartości mniejszej niż 130.000,00 złotych netto wprowadzony uchwałą Zarządu Powiatu w Nowym Mieście Lubawskim nr 195/1244/2024 z dnia 7 marca 2024 r.
3. Oznaczenie wg Wspólnego Słownika Zamówień (kod CPV):

   Część 1. i 2.:

   72800000-8 – Usługi audytu komputerowego i testowania komputerów

   72222200-9 – Usługi w zakresie systemów informacji lub usługi w zakresie planowania technologii

   Część 3.:

   80533100-0 – usługi szkolenia komputerowego
4. Zamawiający dopuszcza składanie ofert częściowych.

   Uwaga: Ten sam Wykonawca nie może realizować części 1. i części 2. zamówienia. Wykonawca może złożyć ofertę na obie te części zamówienia, ale w przypadku, gdy jego oferta zostanie uznana za najkorzystniejszą w części nr 1., oferta tego Wykonawcy na część nr 2. zostanie odrzucona (nawet jeśli będzie najkorzystniejsza). Do realizacji części nr 2. zostanie wtedy wybrany Wykonawca, który złożył drugą w kolejności, najkorzystniejszą ofertę w tej części.
5. Zamawiający nie dopuszcza składania ofert wariantowych.
6. Zamawiający nie przewiduje udzielania zamówień uzupełniających.
7. Postępowanie prowadzone jest w języku polskim, w portalu Baza Konkurencyjności: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl

4. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest przegląd, opracowanie i dostosowanie do nowych wymagań oraz

wdrożenie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w tym m.in. Polityki Bezpieczeństwa Informacji, analizy ryzyka i ciągłości działania, audyt SZBI zgodny z wymaganiami prawnymi, audyt zgodności z wymaganiami Rozporządzenia KRI, potwierdzający zrealizowanie grantu oraz przeprowadzenie szkolenia z zakresu cyberbezpieczeństwa dla wybranych przedstawicieli kadry Starostwa Powiatowego w Nowym Mieście Lubawskim („Urząd"), istotnych z punktu widzenia wdrożonej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji.

Przedmiot zamówienia jest podzielony na 3 części:

- **Część 1.:** Przegląd, opracowanie i dostosowanie do nowych wymagań oraz wdrożenie dokumentacji SZBI.
- **Część 2.:** Audyt SZBI zgodny z wymaganiami prawnymi i audyt zgodności z wymaganiami Rozporządzenia KRI, potwierdzający zrealizowanie grantu.
- **Część 3.:** Szkolenie z zakresu cyberbezpieczeństwa.

Ocena ofert zostanie przeprowadzona dla każdej części z osobna.

Wykonawcy mogą składać oferty na dowolną liczbę części.

5. Wymagania ogólne (do wszystkich części zamówienia)

1. Miejscem realizacji zamówienia są budynki Starostwa Powiatowego w Nowym Mieście Lubawskim, w trzech lokalizacjach:
    1) Budynek główny
       ul. Rynek 1
       13-300 Nowe Miasto Lubawskie
    2) Wydział Geodezji i Nieruchomości
       ul. Grunwaldzka 3
       13-300 Nowe Miasto Lubawskie
    3) Wydział Zarządzania Kryzysowego
       ul. Szkolna 5b
       13-300 Nowe Miasto Lubawskie
2. Szkolenia oraz inne prace wymagające udziału pracowników Starostwa Powiatowego w Nowym Mieście Lubawskim muszą odbywać się w godzinach pracy Urzędu.
3. Wykonawca w ramach wykonania każdej z części zamówienia **przygotuje szczegółowy harmonogram realizacji zamówienia** i przedstawi go Zamawiającemu do akceptacji w terminie

nie dłuższym, niż 5 dni roboczych od podpisania umowy na realizację danej części zamówienia.

4. We wszystkich częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. Zapisy SZBI muszą być otwarte, inkluzywne i niedyskryminujące. W przypadku szkolenia stacjonarnego wykonawca będzie musiał zapewnić materiał szkoleniowy z większym rozmiarem czcionki (w zależności od potrzeb uczestników szkolenia). W ramach grup szkoleniowych przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane dokumenty (w tym dokumentacja SZBI, raporty z audytów i materiały szkoleniowe) będą musiały być dostarczone w formie papierowej i elektronicznej z możliwością powiększania treści. Zamawiający dopuszcza dostarczenie dokumentacji w formie elektronicznej, np. dokumenty w standardzie PDF.
5. Wykonawca zamówienia będzie zobowiązany do podpisania oświadczenia potwierdzającego przestrzeganie powyższych zasad.

5.1. Część 1.: Przegląd, opracowanie i dostosowanie do nowych wymagań oraz wdrożenie dokumentacji SZBI

Starostwo Powiatowe w Nowym Mieście Lubawskim, jako podmiot publiczny, jest zobowiązane do ochrony informacji w organizacji i podlega wymogom dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywy NIS2).

Urząd posiada obecnie Zintegrowany System Zarządzania („ZSZ"), który został opisany w Księdze Zintegrowanego Systemu Zarządzania zatwierdzonej zarządzeniem nr 133/2018 Starosty Nowomiejskiego z dnia 25 maja 2018 roku. ZSZ obejmuje:

- System Zarządzania Jakością („SZJ") zgodny z normą PN-ISO 9001:2015,
- System Zarządzania Bezpieczeństwem Informacji zgodny z normą PN-ISO/IEC 27001:2014,
- Kontrolę Zarządcza („KZ") wynikającą z przepisów ustawy o finansach publicznych.

W ramach ZSZ na SZBI składają się dwa dokumenty: Polityka Bezpieczeństwa Informacji i Polityka

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

zarządzania ryzykiem w bezpieczeństwie informacji oraz zapisy w części ogólnej Księgi ZSZ. Nie stanowią one kompleksowego SZBI i wymagają aktualizacji. Zamawiający zakłada, że docelowy SZBI nie będzie zintegrowany z SZJ i KZ, choć musi uwzględniać ich założenia. Opracowanie i wdrożenie pełnej dokumentacji SZBI z dostosowaniem do aktualnych wymagań pozwoli określić zestaw polityk, procedur, procesów, narzędzi i kompetencji, które wspomogą zwiększyć poziom cyberbezpieczeństwa. W rezultacie ma zostać podniesiony poziom cyberbezpieczeństwa w Urzędzie co ma umożliwić w większym zakresie czerpanie korzyści z cyfryzacji przez Urząd i mieszkańców powiatu. Wdrożenie SZBI ma obejmować mechanizmy monitoringu bezpieczeństwa informacji w Urzędzie.

W ramach realizacji części 1. zamówienia Wykonawca zobowiązany będzie do opracowania dokumentacji SZBI oraz do doradztwa w ustanowieniu i wdrożeniu SZBI w Starostwie Powiatowym w Nowym Mieście Lubawskim, z uwzględnieniem nakładów planowanych do poniesienia w ramach grantu, a w szczególności z uwzględnieniem wykorzystania zakupywanego sprzętu i oprogramowania podnoszącego poziom cyberbezpieczeństwa.

Wykonawca ma za zadanie stworzyć kompleksowy System Zarządzania Bezpieczeństwem Informacji, obejmujący wszystkie niezbędne aspekty, a nie tylko ochronę danych osobowych. Polityka Bezpieczeństwa Informacji musi zostać zaktualizowana. W dokumentacji mają zostać zawarte m.in. zapisy dotyczące reguł współpracy ze stronami trzecimi, w tym z dostawcami, mającymi wpływ na bezpieczeństwo informacji w ramach zlecania wytwarzania oprogramowania i jego utrzymania, w tym dla zapewnienia ciągłości bezpieczeństwa informacji.

Zakres zamówienia obejmuje:

1. Przegląd (tzw. audyt zerowy) istniejącego SZBI (ZSZ) i innych procedur wewnętrznych pod kątem zgodności z obowiązującymi przepisami i normami, istotności w kontekście docelowego SZBI oraz określenia brakującej dokumentacji.
2. Opracowanie nowej/poprawionej dokumentacji SZBI (dedykowane szablony do uzupełnienia przez Zamawiającego).
3. Doradztwo w ustanowieniu i wdrożeniu SZBI, w tym:
   – Omówienie obowiązków wynikających z SZBI,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- Wskazanie działań, jakie musi podjąć Zamawiający w celu wdrożenia SZBI,
- Wskazanie niezbędnego zakresu uzupełnienia dokumentacji przez Zamawiającego,
- Weryfikacja dokumentacji uzupełnionej przez Zamawiającego,
- Instruktaż z szacowania ryzyka,
- Weryfikację szacowania ryzyka przeprowadzonego przez Zamawiającego,
- Instruktaż z inwentaryzacji aktywów informacyjnych,
- Weryfikację wyników inwentaryzacji przeprowadzonej przez Zamawiającego,
- Instruktaż z opracowania upoważnień do przetwarzania informacji
- Weryfikację upoważnień do przetwarzana informacji opracowanych przez Zamawiającego.

4. Udział w audycie SZBI, który zostanie zamówiony w ramach części 2. zamówienia i przeprowadzony przez innego wykonawcę w IV kwartale 2025 roku. Realizacja tego punktu stanowić będzie zobowiązanie gwarancyjne Wykonawcy i nie będzie stanowiła podstawy do żądania dodatkowego wynagrodzenia.

   Jeśli audyt SZBI ujawni nieprawidłowości lub braki wynikające z winy Wykonawcy, będzie on zobowiązany do dostosowania dokumentacji do zaleceń poaudytowych.

Produktem realizacji części 1. zamówienia ma być kompletna dokumentacja SZBI dla Urzędu.

Wymagania dotyczące SZBI

SZBI ma być zgodny z przepisami prawa unijnego (w tym z dyrektywą NIS2), krajowego oraz normami odnoszącymi się do bezpieczeństwa informacji i zarządzania ciągłością działania (w tym: ISO 27001, ISO 27002 dla systemów informatycznych, ISO 22301).

Dokumentacja SZBI musi być opracowana na podstawie:

- Polskiej Normy PN-ISO/IEC 27001 w całości oraz norm powiązanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem,
- Polskiej Normy ISO PN-ISO/ IEC 22301 w całości (opracowanie pełnej dokumentacji) z uwzględnieniem niezbędnych elementów Polskiej Normy PN-ISO/IEC 24762 –

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

5.2. Część 2.: Audyt SZBI zgodny z wymaganiami prawnymi i audyt zgodności z wymaganiami Rozporządzenia KRI, potwierdzający zrealizowanie grantu

W ramach realizacji części 2. zamówienia Wykonawca zobowiązany będzie do wykonania dwóch audytów:

a) audytu Systemu Zarządzania Bezpieczeństwem Informacji zaktualizowanego w ramach części 1. zamówienia, pod względem zgodności systemu z wymogami prawnymi i normami, a w szczególności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077 z późn, zm. – dalej „uoKSC"),

b) audytu zgodności z rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773 – dalej „KRI") oraz z technicznymi wymaganiami wynikającymi z uoKSC, potwierdzającego zrealizowanie grantu na koniec projektu.

Przeprowadzenie audytu SZBI musi pozwolić na weryfikację poprawności stosowanych procedur i zabezpieczeń w odniesieniu do założonych wymagań. Audyt zgodności z KRI ma potwierdzić czy w wyniku realizacji projektu grantowego podniesiony został poziom cyberbezpieczeństwa w Starostwie Powiatowym w Nowym Mieście Lubawskim i czy osiągnięte zostały cele projektu. W wyniku obu audytów mają zostać przygotowane raporty podsumowujące przeprowadzone weryfikacje, zawierające omówienie wszystkich niezgodności.

a) Zakres audytu SZBI

Audyt powinien mieć charakter proceduralny, a jego zakres musi uwzględniać wytyczne normy ISO 27001 oraz specyficzne wymagania proceduralne uoKSC, ze szczególnym naciskiem na obowiązki związane z cyberbezpieczeństwem, zarządzaniem ryzykiem oraz reakcją na incydenty. Zakres audytu:

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

I. Audyt organizacyjny

Audyt organizacyjny obejmuje:

1. Weryfikację regulacji wewnętrznych Zamawiającego w obszarze zarządzania bezpieczeństwem informacji oraz procedur ich audytów i aktualizacji, w tym zgodności z normą ISO 27001 oraz z uoKSC:
   - Zasady postępowania z informacjami, w szczególności zapewniające minimalizację ryzyka kradzieży informacji, nieuprawnionego dostępu, uszkodzeń, zakłóceń oraz kradzieży środków przetwarzania informacji, w tym urządzeń mobilnych.
   - Procedury zgłaszania incydentów bezpieczeństwa, uwzględniające obowiązek raportowania incydentów do odpowiednich zespołów CSIRT, w tym określenie reakcji na różne typy zagrożeń.
   - Zasady reagowania na podatności systemów teleinformatycznych: analiza procedur działania w przypadku wykrycia lub publikacji informacji o podatnościach technicznych systemów oraz w zakresie współpracy z podmiotami odpowiedzialnymi za cyberbezpieczeństwo.
   - Zasady dostępu do systemów operacyjnych: weryfikacja polityk kontroli dostępu oraz zabezpieczeń przed nieautoryzowanymi instalacjami oprogramowania.
   - Procedury audytu wewnętrznego i aktualizacji dokumentacji.
2. Weryfikację odpowiedzialności i uprawnień pracowników w zakresie zarządzania bezpieczeństwem informacji, w tym danych osobowych, zgodnie z wymaganiami SZBI oraz uoKSC, z uwzględnieniem odpowiednich szkoleń oraz certyfikacji.
3. Weryfikację procedur zmiany uprawnień w przypadku rotacji kadr i/lub zmiany zadań pracowników, zgodnie z wymogami SZBI oraz uoKSC, obejmującą procedury nadawania, modyfikowania i odbierania dostępu do informacji wrażliwych.
4. Analizę dokumentacji dotyczącej bezpieczeństwa informacji w kontekście zawierania umów

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

wykonawczych i serwisowych, zgodnie z wymaganiami SZBI oraz uoKSC, z uwzględnieniem odpowiednich klauzul ochrony danych i odpowiedzialności stron trzecich za naruszenia bezpieczeństwa.

5. Analizę ryzyka: weryfikację procedur analizy ryzyka utraty integralności, dostępności i poufności informacji zgodnie z wymogami SZBI oraz uoKSC, w tym ocenę mechanizmów aktualizacji tej analizy oraz stosowania odpowiednich środków zaradczych.

6. Weryfikację polityki zapewnienia ciągłości działania i planów awaryjnych.

II. Audyt fizyczny i środowiskowy

Audyt fizyczny i środowiskowy należy przeprowadzić we wszystkich trzech lokalizacjach Starostwa Powiatowego w Nowym Mieście Lubawskim. Audyt obejmuje:

1. Weryfikację granic obszaru bezpiecznego, obejmującą fizyczne granice miejsc, gdzie przetwarzane są informacje wrażliwe, oraz dostępność i funkcjonalność zabezpieczeń fizycznych.

2. Zabezpieczenia wejścia/wyjścia: procedury kontroli dostępu do pomieszczeń (np. serwerowni i archiwów) i autoryzacji.

3. Procedury zarządzania bezpieczeństwem fizycznym, w tym monitorowania dostępu i ochrony przed zagrożeniami fizycznymi.

4. Procedury zapewnienia ciągłości działania i zabezpieczeń infrastruktury fizycznej, w tym wymagania w zakresie zasilania awaryjnego, procedury zarządzania awariami, itp.

b) Zakres audytu zgodności z KRI

Audyt powinien mieć charakter proceduralny, a jego zakres musi uwzględniać specyficzne wymagania KRI i techniczne wymagania wynikające z uoKSC oraz koncentrować się na zabezpieczeniach infrastruktury IT, systemach teleinformatycznych, bezpieczeństwie sieci i systemów. Zakres audytu:

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

I. Audyt organizacyjny

Audyt organizacyjny obejmuje:

1. Weryfikację zgodności polityki bezpieczeństwa informacji z KRI, w tym:
   - Zasady bezpiecznej pracy mobilnej i pracy zdalnej, uwzględniające środki techniczne i organizacyjne chroniące przed zagrożeniami wynikającymi z pracy na odległość, w tym politykę haseł oraz ochronę połączeń zdalnych.
2. Weryfikację stosowania procedur zmiany uprawnień w przypadku rotacji kadi i/lub zmiany zadań pracowników, obejmującą procedury nadawania, modyfikowania i odbierania dostępu do informacji wrażliwych.
3. Weryfikację zgodności procedur zarządzania IT z minimalnymi wymaganiami KRI.

II. Audyt teleinformatyczny

Audyt teleinformatyczny należy przeprowadzić we wszystkich trzech lokalizacjach Starostwa Powiatowego w Nowym Mieście Lubawskim. Audyt obejmuje:

1. Weryfikację stosowania procedur zarządzania, konfiguracji i zabezpieczeń systemów teleinformatycznych: zgodność KRI w zakresie zarządzania bezpieczeństwem systemów, w tym aktualizacji, monitorowania i reagowania na incydenty.
2. Przegląd zasobów informatycznych oraz rozwiązań dla zapewnienia ciągłości działania:
   - Minimalizowanie ryzyka utraty informacji w wyniku awarii: analiza kopii zapasowych i procedur ich testowania, redundancji zasobów, systemów podtrzymania zasilania, chłodzenia oraz alarmów i przywracania działania systemów po incydencie.
   - Ochrona przed błędami, utratą, ujawnieniem, nieuprawnioną modyfikacją danych, bezpieczeństwo sieci wewnętrznej, komputerów, urządzeń mobilnych oraz metod zapobiegania nieautoryzowanym operacjom: zgodność z KRI. Stosowanie mechanizmów kryptograficznych: ocena wdrożonych rozwiązań kryptograficznych zgodnych z uoKSC i KRI.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- Bezpieczeństwo plików systemowych: weryfikacja zgodności z wymogami zabezpieczeń systemowych.
- Weryfikacja zabezpieczeń antywirusowych.
- Weryfikacja zabezpieczeń przed nieautoryzowanym dostępem, w tym urządzeń firewall i/lub UTM.
- Weryfikacja systemów monitorowania i reagowania na incydenty (SIEM, IDS/IPS) i/lub usług centrów monitorowania bezpieczeństwa (SOC).

3. Zarządzanie aktualizacjami oprogramowania: weryfikację procedur zarządzania aktualizacjami oprogramowania, zgodnie z KRI, w tym automatyzacji i monitorowania procesu aktualizacji.
4. Zabezpieczenia stacji roboczych i nośników danych: weryfikację bezpieczeństwa stacji roboczych i nośników danych, w tym ich szyfrowania i fizycznej ochrony, zgodnie z uoKSC i KRI.
5. Weryfikację stosowania polityki haseł: zgodność stosowanych polityk tworzenia, przechowywania i zmiany haseł z wymogami KRI i uoKSC, w tym zabezpieczeń przed nieautoryzowanym dostępem.
6. Weryfikację fizycznych zabezpieczeń urządzeń oraz pomieszczeń, w tym dostępności systemów monitoringu i alarmowych.
7. Audytowi podlega całość sprzętu informatycznego będącego w posiadaniu Zamawiającego (w tym sprzęt nabywany w ramach grantu):
   - serwery fizyczne – 8 szt. (w tym dwa klastry po dwa serwery),
   - serwery wirtualne – 8 szt.,
   - komputery stacjonarne – 48 szt.,
   - notebooki – 20 szt.,
   - drukarki sieciowe – 12 szt.,
   - urządzenia UTM – 3 szt.,
   - macierze dyskowe – 4 szt.,
   - dyski sieciowe NAS – 3 szt.,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- sieci lokalne (fizyczne) – 2,
- podsieci lokalne – 1,
- łącza do Internetu – 3.,
- liczba zewnętrznych numerów IP – 3,
- Active Directory – 2.

Dokumentacja poaudytowa

Po zakończeniu każdego z audytów Wykonawca przygotuje raport zawierający wnioski dotyczące stanu obecnego, wytyczne do dalszego doskonalenia i rekomendacje w zakresie poprawy cyberbezpieczeństwa w SP na przyszłość. Dokumentacje poaudytowe muszą obejmować co najmniej:

- Wprowadzenie (cel audytu, zakres, kluczowe obszary audytowane, datę przeprowadzenia audytu, opis jednostek, systemów, procedur i obszarów objętych audytem),
- Opis zastosowanych metod i działań audytowych,
- Ocenę zgodności z przepisami: Ogólna ocena stopnia zgodności odpowiednio z uoKSC, KRI oraz innymi regulacjami i normami, takimi jak RODO lub ISO 27001,
- Identyfikację niezgodności: Wyszczególnienie obszarów, w których audyt wykazał brak zgodności z wymaganiami prawnymi lub procedurami wewnętrznymi. Każda niezgodność powinna być opisana i sklasyfikowana (np. krytyczna, wysoka, średnia, niska),
- Wyniki audytu, w tym:
    - opis mocnych stron – obszarów, w których SP spełnia wymogi i wykazuje się dobrymi praktykami w zakresie zarządzania bezpieczeństwem informacji,
    - wskazanie słabych punktów – wykrytych podatności, niezgodności lub braków w procedurach oraz zabezpieczeniach technicznych i organizacyjnych,
    - ocenę ryzyka – analizę wykrytych ryzyk związanych z bezpieczeństwem informacji, obejmującą ryzyka dla integralności, poufności i dostępności danych oraz systemów.
- Rekomendacje i zalecenia audytorów zawierające:
    - zalecane działania naprawcze (np. wzmocnienie polityk bezpieczeństwa, poprawę lub wprowadzenie procedur reagowania na incydenty, dostosowanie zabezpieczeń technicznych i organizacyjnych),
    - priorytetyzację działań (np. podział działań na krytyczne, pilne, zalecane), aby

umożliwić organizacji skuteczne planowanie działań naprawczych,

- propozycję terminów realizacji działań naprawczych,
- sugerowane terminy przyszłych audytów lub działań kontrolnych w celu zapewnienia ciągłej zgodności.

– Podpisy i oświadczenia audytorów (np. o rzetelności przeprowadzonego audytu i pełnym przedstawieniu wyników oraz wniosków).
– Załączniki (np. listę uczestników audytu, listę przeanalizowanych dokumentów, polityk i procedur, listę sprzętu, konfigurację sieci).

5.3. Część 3.: Szkolenie z zakresu cyberbezpieczeństwa

W ramach realizacji części 3. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia szkolenia stacjonarnego dla wybranych przedstawicieli kadry Starostwa Powiatowego w Nowym Mieście Lubawskim, istotnych z punktu widzenia wdrożonej polityki bezpieczeństwa informacji i Systemu Zarządzania Bezpieczeństwem Informacji. Pracownicy odbyli w listopadzie 2024 roku podstawowe szkolenie budujące świadomość cyberzagrożeń i sposobów ochrony. Celem szkolenia zamawianego w ramach części 3. zamówienia jest podniesienie poziomu wiedzy i kompetencji kadry JST z zakresu cyberbezpieczeństwa przede wszystkim z punktu widzenia SZBI wdrażanej w ramach części 1. zamówienia i ról, które poszczególne osoby pełnią w ramach SZBI.

Nacisk ma zostać położony na podniesienie świadomości zagrożeń i reakcji osób posiadających wyznaczone obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami, umiejętność oceny sytuacji naruszenia cyberbezpieczeństwa, identyfikację prób ataków (w tym ataków socjotechnicznych) i podejmowania odpowiednich kroków w celu ich zneutralizowania oraz na podejmowane działania i postępowanie zgodnie z procedurami i rolami w SZBI. Szkolenie ma być zorientowane na praktyczne wykorzystanie wiedzy zdobytej podczas kursu.

Szkolenie ma obejmować **ćwiczenia praktyczne (min. 25% czasu trwania szkolenia)**, pozwalające na podniesienie umiejętności związanych z:

– rozpoznawaniem zagrożeń,
– oceną sytuacji,
– identyfikacją prób ataków,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- reagowaniem na zagrożenia i naruszenia,
- podejmowanie działań zgodnych z procedurami SZBI i rolami poszczególnych osób,
- zarządzaniem w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).

W wyniku szkolenia pracownicy Urzędu mają znać zasady ochrony danych osobowych i wrażliwych informacji zgodnie z przepisami, oraz być świadomi swojej roli w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) i umieć podejmować odpowiednie działania.

Wymagana forma przeprowadzenia szkolenia: **szkolenie stacjonarne**. Zamawiający zapewni salę szkoleniową na maksymalnie 25 osób z ekranem, rzutnikiem i flipchartem. Wykonawca musi zapewnić komputery do ćwiczeń praktycznych.

W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający dopuszcza dostarczenie kompletu materiałów w formie elektronicznej, np. dokumenty w standardzie PDF.

Liczba osób do przeszkolenia – 25.

Czas trwania szkolenia – min. 8 godzin lekcyjnych (po 45 min.).

Liczba edycji szkolenia – 1

W terminie wynikającym ze szczegółowego harmonogramu realizacji zamówienia opracowanego przez Wykonawcę, Wykonawca opracuje program szkolenia, który musi zawierać **informacje dotyczące tematyki i czasu szkolenia (w tym ćwiczeń)** i przedstawi go Zamawiającemu do akceptacji.

Program szkolenia może zostać zmodyfikowany i musi odnosić się do aktualnych zagrożeń cyberbezpieczeństwa z punktu widzenia wdrożonej polityki bezpieczeństwa informacji i Systemu Zarządzania Bezpieczeństwem Informacji.

Z przeprowadzonego szkolenia Wykonawca musi przedstawić **listy obecności** z podpisami uczestników szkolenia. Każdy uczestnik szkolenia musi otrzymać od Wykonawcy imienny certyfikat z podpisem trenera, potwierdzający ukończenie szkolenia i jego zakres.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Szkolenie musi być zakończone **anonimową ankietą** wśród uczestników, oceniającą co najmniej przydatność szkolenia, zakres przekazanych informacji, adekwatność przekazanych informacji do potrzeb uczestników, formę prezentacji i komunikatywność prowadzącego szkolenie. Wykonawca przedstawi Zamawiającemu **podsumowanie wyników ankiety**.

6. Termin realizacji zamówienia

Zamówienie (wszystkie części) musi zostać zrealizowane nie później niż do 31 marca 2026 r.

Terminy realizacji poszczególnych części:

1. **Część 1.: Przegląd, opracowanie i dostosowanie do nowych wymagań oraz wdrożenie dokumentacji SZBI:**
   - w ciągu 90 dni od daty podpisania umowy na realizację.
2. **Część 2.: Audyt SZBI zgodny z wymaganiami prawnymi i audyt zgodności z wymaganiami Rozporządzenia KRI, potwierdzający zrealizowanie grantu:**
   - Audyt SZBI zgodny z wymaganiami prawnymi – IV kwartał 2025 r.,
   - Audyt zgodności z wymaganiami Rozporządzenia KRI – I kwartał 2026 r.
3. **Część 3.: Szkolenie z zakresu cyberbezpieczeństwa:**
   - III kwartał 2025 r.

UWAGA! Dokładne terminy realizacji poszczególnych części zamówienia zostaną uzgodnione pomiędzy Zamawiającym i Wykonawcą.

7. Warunki płatności

Część 1. i część 3.: Płatność po wykonaniu każdej z części zamówienia w całości.

Część 2.: Płatności częściowe po wykonaniu każdego z audytów.

Termin płatności – 30 dni od dnia dostarczenia do siedziby Zamawiającego poprawnie wystawionej faktury VAT.

8. Warunki udziału w postępowaniu

O udzielenie zamówienia mogą ubiegać się Wykonawcy nie podlegający wykluczeniu i spełniający warunki udziału w postępowaniu, dotyczące **zdolności technicznej lub zawodowej**, którzy:

dla części 1.:

1. mają co najmniej 2-letnie doświadczenie w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) w opracowywaniu lub aktualizacji Systemów Zarządzania Bezpieczeństwem Informacji (data rozpoczęcia realizacji co najmniej jednego z wykazywanych zamówień musi być ponad dwa lata wcześniejsza od terminu składania ofert),
2. zrealizowali w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) co najmniej 2 zamówienia polegające na opracowaniu lub przeglądzie i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach sektora finansów publicznych, w tym 1 (jedno) zamówienie w urzędzie administracji rządowej lub samorządowej,
3. dysponują lub będą dysponować co najmniej 2 audytorami, którzy będą uczestniczyć w realizacji zamówienia, z których każdy:
   - ma wykształcenie wyższe,
   - posiada certyfikat audytora wiodącego ISO/IEC 27001 w wersji 2007 albo nowszej lub inny certyfikat wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
   - posiada co najmniej 2-letnie doświadczenie w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) w opracowywaniu lub aktualizacji Systemów Zarządzania Bezpieczeństwem Informacji (data rozpoczęcia realizacji co najmniej jednego z wykazywanych zamówień musi być ponad dwa lata wcześniejsza od terminu składania ofert),
   - brał udział w realizacji co najmniej 2 zamówień polegających na opracowaniu lub przeglądzie i aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach sektora finansów publicznych, w tym 1 (jedno) zamówienie w urzędzie administracji rządowej lub samorządowej.

dla części 2.:

1. mają co najmniej 2-letnie doświadczenie w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) w prowadzeniu audytów cyberbezpieczeństwa (data rozpoczęcia realizacji co najmniej jednego z wykazywanych zamówień musi być ponad dwa lata wcześniejsza od terminu składania ofert),
2. zrealizowali w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) co najmniej

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

3 zamówienia polegające na przeprowadzeniu audytu cyberbezpieczeństwa w zakresie zgodności z uoKSC i KRI, obejmujące co najmniej audyt organizacyjny, audyt fizyczny i środowiskowy oraz audyt teleinformatyczny w urzędach administracji rządowej lub samorządowej,

3. zrealizowali w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) co najmniej 1 zamówienie polegające na przeprowadzeniu audytu Systemu Zarządzania Bezpieczeństwem Informacji,
4. dysponują lub będą dysponować co najmniej 2 audytorami, którzy będą uczestniczyć w realizacji zamówienia, z których każdy:
   - ma wykształcenie wyższe,
   - posiada certyfikat audytora wiodącego ISO/IEC 27001 w wersji 2007 albo nowszej lub inny certyfikat wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
   - posiada co najmniej 2-letnie doświadczenie w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) w prowadzeniu audytów cyberbezpieczeństwa (data rozpoczęcia realizacji co najmniej jednego z wykazywanych zamówień musi być ponad dwa lata wcześniejsza od terminu składania ofert),
   - brał udział w realizacji co najmniej 3 audytów cyberbezpieczeństwa w zakresie zgodności z uoKSC i KRI, obejmujących co najmniej audyt organizacyjny, audyt fizyczny i środowiskowy oraz audyt teleinformatyczny w urzędach administracji rządowej lub samorządowej.

Uwaga: Ten sam Wykonawca nie może realizować części 1. i części 2. zamówienia. Wykonawca może złożyć ofertę na obie te części zamówienia, ale w przypadku, gdy jego oferta zostanie uznana za najkorzystniejszą w części nr 1., oferta tego Wykonawcy na część nr 2. Zostanie odrzucona (nawet jeśli będzie najkorzystniejsza). Do realizacji części nr 2. zostanie wtedy wybrany Wykonawca, który złożył drugą w kolejności, najkorzystniejszą ofertę w tej części.

dla części 3.:

1. mają co najmniej 2-letnie doświadczenie w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) w przygotowaniu i przeprowadzeniu szkoleń z zakresu cyberbezpieczeństwa (data rozpoczęcia realizacji co najmniej jednego z wykazywanych szkoleń musi być ponad dwa lata

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

wcześniejsza od terminu składania ofert),

2. zrealizowali w okresie od 19 lipca 2021 r. (inauguracja konkursu grantowego) przynajmniej 3 zamówienia obejmujące wykonanie szkoleń z zakresu cyberbezpieczeństwa w urzędach administracji rządowej lub samorządowej,
3. dysponują lub będą dysponować co najmniej 2 trenerami, którzy będą uczestniczyć w realizacji zamówienia, z których każdy:
   - ma wykształcenie wyższe,
   - posiada certyfikat audytora wiodącego ISO/IEC 27001 w wersji 2007 lub nowszej lub inny certyfikat wymieniony w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
   - posiada co najmniej 2 letnie doświadczenie liczone od dnia 19 lipca 2021 r. (inauguracja konkursu grantowego) w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa (data rozpoczęcia realizacji co najmniej jednego z wykazywanych szkoleń musi być ponad dwa lata wcześniejsza od terminu składania ofert) oraz przeprowadził w tym okresie przynajmniej 30 godzin (zegarowych) szkoleń na temat cyberbezpieczeństwa w urzędach administracji rządowej lub samorządowej.

Na potwierdzenie spełnienia ww. warunków Wykonawca zobowiązany jest przedstawić do każdej części postępowania:

- **wykaz usług** zrealizowanych w okresie od dnia 19 lipca 2021 r. (inauguracja konkursu grantowego) wraz z dokumentami potwierdzającym należytą realizację zamówień (np. listy referencyjne, protokoły odbiorów bez uwag) – wzór wykazu stanowi **załącznik nr 3.** do niniejszego zapytania ofertowego.
- **wykaz osób** przeznaczonych do realizacji zamówienia publicznego, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień i doświadczenia niezbędnego do wykonania zamówienia, a także kopiami dokumentów potwierdzających posiadane doświadczenie i certyfikaty – wzór wykazu stanowi **załącznik nr 4.** do niniejszego zapytania ofertowego.

Oferty Wykonawców nie spełniających ww. warunków nie będą rozpatrywane.

Zamawiający zastrzega sobie prawo sprawdzania w toku oceny ofert wiarygodności przedstawionych przez Wykonawcę dokumentów, wykazów, danych i informacji.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

9. Wykluczenie z udziału w postępowaniu

1. Z postępowania o udzielenie zamówienia wyklucza się Wykonawców:
   1) będących osobami fizycznymi, które prawomocnie skazano za:
      a) udział w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      b) handel ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      c) przestępstwo o którym mowa w art. 228-230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
      d) finansowanie przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
      e) przestępstwo o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
      f) powierzenie wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
      g) przestępstwo przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
      h) przestępstwo o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

2) będących spółkami prawa handlowego jeżeli urzędującego członka ich organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt. 1);
3) wobec których wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec których prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5) co do których Zamawiający, na podstawie wiarygodnych przesłanek, może stwierdzić że zawarli z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz.U. 2024 poz. 594 z późn. zm.), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
6) o których mowa w art. 85 ust. 1 p.z.p., jeśli doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tych Wykonawców lub podmiotów, które należy z tymi Wykonawcami do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity: Dz.U. 2024 poz. 594 z późn. zm.), chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie tych Wykonawców z udziału w postępowaniu o udzielenie zamówienia.

2. Zamawiający nie przewiduje wykluczenia Wykonawców, o których mowa w art. 109 ust.1 p.z.p.
3. Wykluczenie Wykonawcy następuje zgodnie z art. 111 p.z.p.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

4. Zgodnie z zapisami art. 1 pkt 3) oraz art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (tekst jednolity: Dz.U. 2024 poz. 507) z postępowania wyklucza się:
   1) Wykonawcę wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
   2) Wykonawcę, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1285, 1723 i 1843) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3;
   3) Wykonawcę, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3.
5. Zamawiający wykluczy z postępowania Wykonawcę, który jest powiązany z Zamawiającym osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między beneficjentem lub osobami upoważnionymi do zaciągania zobowiązań w imieniu beneficjenta lub osobami wykonującymi w imieniu beneficjenta czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:
   1) uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej,
   2) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów

prawa,

3) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
4) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli albo pozostawanie z nimi we wspólnym pożyciu przez Wykonawcę, jego zastępcę prawnego lub członków organów zarządzających lub organów nadzorczych Wykonawcy,
5) pozostawanie z nimi w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

6. Weryfikacji braku podstawy wykluczenia, o której mowa w ust. 4, w stosunku do konkretnego podmiotu zamawiający może dokonać w dowolnym czasie, za pomocą wszelkich dostępnych środków.

10. Sposób przygotowania oferty

1. Ofertę należy sporządzić na formularzu ofertowym stanowiącym **załącznik nr 1.** do niniejszego zapytania ofertowego.
2. Do oferty musi zostać załączony oświadczenie o braku powiązań z Zamawiającym i braku podstaw do wykluczenia stanowiące **załącznik nr 2.** do niniejszego zapytania ofertowego wykaz usług stanowiący **załącznik nr 3.** oraz wykaz osób przeznaczonych do realizacji zamówienia stanowiący **załącznik nr 4.**
3. Cena oferty musi być ceną ryczałtową, obejmować całość zamówienia i być podana w złotych polskich.
4. Oferta winna być podpisana przez osobę/y upoważnione do reprezentowania Wykonawcy.
5. Ofertę należy podpisać podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu, podpisem zaufanym lub podpisem osobistym.
6. Wszelkie dokumenty, w tym certyfikaty i dokumenty potwierdzające należytą realizację zamówień, sporządzone w postaci papierowej muszą zostać dostarczone w postaci kopii (skanów) potwierdzonych przez Wykonawcę za zgodność z oryginałem za pomocą podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu, podpisu zaufanego lub podpisu

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

osobistego. Dokumenty sporządzone w postaci elektronicznej muszą zostać dostarczone z oryginalnymi podpisami elektronicznymi, którymi zostały opatrzone.

7. Oferta winna być sporządzona w języku polskim pod rygorem nieważności. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem przysięgłym na język polski.
8. Wykonawca ma prawo złożyć tylko 1 ofertę. Złożenie przez Wykonawcę więcej niż 1 oferty, skutkuje odrzuceniem wszystkich ofert złożonych przez tego Wykonawcę.
9. Wszelkie koszty przygotowania oferty ponosi Wykonawca.
10. Nie przewiduje się zwrotu kosztów udziału w postępowaniu.
11. Termin związania ofertą wynosi 30 dni.
12. Wykonawca informuje Zamawiającego o informacjach zawartych w ofercie stanowiących tajemnicę przedsiębiorstwa.

11. Wymagane dokumenty

Wraz z ofertą Wykonawca jest zobowiązany złożyć dokumenty potwierdzające należytą realizację zamówień wymienionych w wykazie usług oraz dokumenty potwierdzające wykształcenie i certyfikaty potwierdzające posiadanie przez audytorów uprawnień, np. certyfikaty audytora wiodącego ISO/IEC 27001 w wersji 2007 albo nowszej lub inne certyfikaty wymienione w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999).

12. Miejsce i termin składania ofert:

13. Ofertę wraz z załącznikami należy złożyć za pośrednictwem portalu Baza Konkurencyjności – https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl **w terminie do dnia 07.03.2025 r. do godziny 10:00.**
14. O terminowym złożeniu oferty decyduje data złożenia oferty za pośrednictwem portalu Baza Konkurencyjności.
15. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
16. Ofertę wraz z załącznikami składa się, pod rygorem nieważności, w postaci elektronicznej **podpisanej kwalifikowanym podpisem elektronicznym, podpisem zaufanym** lub **podpisem osobistym** przez osobę/y upoważnioną/e do reprezentowania wykonawcy. Brak podpisu/ów w

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

wymieniony sposób będzie skutkował odrzuceniem oferty.

17. **Zamawiający nie dopuszcza innej formy i sposobu składania ofert niż za pośrednictwem portalu Baza Konkurencyjności**. Niespełnienie tego wymogu oznacza niezgodność oferty z Zapytaniem. Oferty złożone w inny sposób zostaną odrzucone przez Zamawiającego.

13. Kryteria wyboru oferty

1. Przy wyborze oferty Zamawiający będzie się kierował następującym kryterium:

   cena brutto – 100%

   Wybrana zostanie oferta z największą ilością punktów spośród ofert nieodrzuconych, obliczoną zgodnie z poniżej określonym wzorem:

$$\frac{\text{Najniższa cena spośród ofert nieodrzuconych}}{\text{Cena oferty badanej}} \times 100$$

2. W sytuacji gdy cena najkorzystniejszej oferty będzie znacząco przewyższała środki zabezpieczone przez Zamawiającego w budżecie, Zamawiający zastrzega sobie możliwość przeprowadzenia dodatkowych negocjacji z Wykonawcą który złoży najkorzystniejszą ofertę.
3. Ten sam Wykonawca nie może realizować części 1. i części 2. zamówienia. Wykonawca może złożyć ofertę na obie te części zamówienia, ale w przypadku, gdy jego oferta zostanie uznana za najkorzystniejszą w części nr 1., oferta tego Wykonawcy na część nr 2. Zostanie odrzucona (nawet jeśli będzie najkorzystniejsza). Do realizacji części nr 2. zostanie wtedy wybrany Wykonawca, który złożył drugą w kolejności, najkorzystniejszą ofertę w tej części.
4. W przypadku gdy wybrany Wykonawca odstąpi od podpisania umowy z Zamawiającym, możliwe jest podpisanie przez Zamawiającego umowy z kolejnym Wykonawcą, który w postępowaniu uzyskał kolejną najwyższą liczbę punktów.
5. Zamawiający może w toku badania i oceny ofert żądać od Oferentów dodatkowych wyjaśnień dotyczących treści złożonych ofert.
6. Zamawiający wyjaśni i poprawi w formularzu ofertowym:
   - oczywiste omyłki pisarskie,
   - oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   - inne omyłki polegające na niezgodności oferty z opisem zawartym w zapytaniu

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

ofertowym niepowodujące istotnych zmian w treści oferty.

7. Poprawienie przez Zamawiającego oczywistych omyłek pisarskich oraz rachunkowych i konsekwencji rachunkowych dokonanych poprawek nie wymaga uzyskania zgody Wykonawcy. Wykonawca może nie wyrazić zgody na poprawienie przez Zamawiającego innych omyłek polegających na niezgodności oferty z opisem zawartym w zapytaniu ofertowym niepowodujące istotnych zmian w treści oferty. Brak zgody Wykonawca musi wnieść na piśmie w wyznaczonym przez Zamawiającego terminie.
8. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, bez podania przyczyny, na każdym etapie prowadzonego postępowania. Z tytułu unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.

14. Kontakt z Zamawiającym

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji między Zamawiającym a Wykonawcą oraz przekazywanie dokumentów i oświadczeń odbywa się pisemnie za pomocą portalu Bazy Konkurencyjności
2. Po stronie Zamawiającego osobą do kontaktów w sprawie zamówienia jest:

   Beata Widźgowska
   Naczelnik Wydziału Inwestycji Mienia i Spraw Gospodarczych
   tel.: +48 56 47 24 212
   e-mail: zamowienia@powiat-nowomiejski.pl

3. W tytule wiadomości należy wskazać numer zapytania ofertowego – GM.272.2.1.2025.
4. Każdy Wykonawca ma prawo zwrócić się do Zamawiającego o wyjaśnienie treści zapytania ofertowego. Pytania wykonawców muszą być przekazane za pośrednictwem portalu Baza Konkurencyjności.
5. Zamawiający udzieli odpowiedzi najpóźniej na 2 dni przed upływem terminu składania ofert pod warunkiem, że wniosek o wyjaśnienie treści zapytania ofertowego wpłynął do Zamawiającego nie później niż 4 dni przed upływem terminu składania ofert.
6. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 5, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych Wykonawców

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia oferty.

7. W przypadku, gdy wniosek o wyjaśnienie treści zapytania ofertowego nie wpłynął w terminie, o którym mowa w ust. 5, Zamawiający nie ma obowiązku udzielania wyjaśnień oraz obowiązku przedłużania terminu składania ofert.

15. Wyjaśnienia oraz uzupełnienia do oferty

1. W toku badania ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonej oferty, treści oświadczeń, dokumentów, pełnomocnictw i ich uzupełnienia.
2. Jeżeli zaoferowana cena będzie rażąco niska w stosunku do przedmiotu zamówienia lub będzie budziła wątpliwości co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający zwróci się do Wykonawcy o udzielenie wyjaśnień, w tym złożenie dowodów dotyczących wyliczenia ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu będzie spoczywać na Wykonawcy.
3. Zamawiający odrzuci ofertę Wykonawcy, który nie udzieli wyjaśnień, o których mowa powyżej lub jeżeli dokonana ocena tych wyjaśnień wraz ze złożonymi dowodami potwierdzi, że zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

16. Klauzula informacyjna RODO

W celu wykonania obowiązku nałożonego w drodze art. 13 i 14 RODO, w związku z art. 88 ustawy wdrożeniowej, informujemy o zasadach przetwarzania Państwa danych osobowych:

Administrator danych

Odrębnymi administratorami Państwa danych są:

1. Minister Funduszy i Polityki Regionalnej (dalej jako MFiPR), w zakresie w jakim pełni funkcję Instytucji Zarządzającej (IZ) Funduszami Europejskimi na Rozwój Cyfrowy 2021-2027 (dalej jako FERC) z siedzibą przy ul. Wspólnej 2/4, 00-926 Warszawa,
2. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Instytucji Pośredniczącej (IP) FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa,
3. Centrum Projektów Polska Cyfrowa (dalej jako CPPC) w zakresie w jakim pełni funkcje Beneficjenta FERC, z siedzibą przy ul. Spokojnej 13A, 01-044 Warszawa.

Cel przetwarzania danych

Państwa dane osobowe będziemy przetwarzać w związku z realizacją FERC, w szczególności w związku z naborem 2.2 FERC. Podanie danych jest dobrowolne, ale konieczne do realizacji ww. celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań.

Podstawa przetwarzania

Będziemy przetwarzać Państwa dane osobowe w związku z tym, że:

1. Zobowiązuje nas do tego prawo (art. 6 ust. 1 lit. c RODO):
   1) art. 87 ustawy wdrożeniowej,
   2) art. 61 ustawy z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r. poz. 1079),
   3) ustawa z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (tekst jednolity Dz.U. z 2023 r. poz. 775 z późn. zm.),
   4) art. 206 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (tekst jednolity Dz. U. z 2022 r. poz. 1634, z późn. zm.),
   5) Porozumienie trójstronne w sprawie systemu realizacji programu „Fundusze Europejskie na Rozwój Cyfrowy 2021-2027" z 2.02.2023 r.,
   6) rozporządzenia Ministra Cyfryzacji z dnia 16 lutego 2023 r. w sprawie udzielania pomocy na rozwój infrastruktury szerokopasmowej w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (Dz. U. z 2023 r. poz. 405),
2. Wykonujemy zadania w interesie publicznym lub sprawujemy powierzoną nam władzę publiczną (art. 6 ust. 1 lit. e RODO),
3. Przygotowujemy i realizujemy umowy, których są Państwo stroną, a przetwarzanie danych osobowych jest niezbędne do ich zawarcia i wykonania (art. 6 ust. 1 lit. b RODO).

Rodzaje przetwarzanych danych

Możemy przetwarzać następujące rodzaje Państwa danych:

1. dane identyfikacyjne, wskazane w art. 87 ust. 2 pkt 1 ustawy wdrożeniowej, w tym: imię, nazwisko, adres, adres poczty elektronicznej, numer telefonu, numer faksu, PESEL, REGON, wykształcenie, identyfikatory internetowe,
2. dane związane z zakresem uczestnictwa osób fizycznych w projekcie, wskazane w art. 87 ust. 2 pkt 2 ustawy wdrożeniowej, w tym w szczególności: wynagrodzenie, formę i okres

zaangażowania w projekcie,

3. dane osób fizycznych widniejące na dokumentach potwierdzających kwalifikowalność wydatków, wskazane w art. 87 ust. 2 pkt. 3 ustawy wdrożeniowej, m.in. numer rachunku bankowego, doświadczenie zawodowe, numer uprawnień budowlanych, numer księgi wieczystej,
4. dane dotyczące wizerunku i głosu osób uczestniczących w realizacji Programu lub biorących udział w wydarzeniach z nim związanych.

Dane pozyskujemy bezpośrednio od osób, których one dotyczą, albo od instytucji i podmiotów zaangażowanych w realizację FERC w tym w szczególności od wnioskodawców, beneficjentów, partnerów.

Dostęp do danych osobowych

Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy MFiPR oraz CPPC.

Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane:

1. podmiotom, w tym ekspertom, o których mowa w art. 80 ustawy wdrożeniowej, którym zleciliśmy wykonywanie zadań w ramach realizacji FERC,
2. instytucji audytowej, o której mowa w art. 71 rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej,
3. instytucjom Unii Europejskiej (UE) lub podmiotom, którym UE powierzyła zadania dotyczące wdrażania FERC;
4. podmiotom, które wykonują dla nas usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym.

Okres przechowywania danych

Będziemy przechowywać Państwa dane osobowe zgodnie z przepisami o narodowym zasobie archiwalnym i archiwach, do momentu zakończenia realizacji przez IZ/IP/Beneficjenta wszelkich zadań związanych z realizacją i rozliczeniem FERC, z zastrzeżeniem przepisów, które mogą przewidywać dłuższy termin przeprowadzania kontroli, a ponadto przepisów dotyczących pomocy publicznej i pomocy de minimis oraz przepisów dotyczących podatku od towarów i usług.

Prawa osób, których dane dotyczą

Przysługują Państwu następujące prawa:

1. dostępu do swoich danych osobowych oraz otrzymania ich kopii (art. 15 RODO),
2. do sprostowania swoich danych (art. 16 RODO),
3. do usunięcia swoich danych (art. 17 RODO) – jeśli dotyczy,
4. do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO),
5. wniesienia sprzeciwu – wobec przetwarzania swoich danych (art. 21 RODO) – jeśli przetwarzanie odbywa się w celu wykonywania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, powierzonej administratorowi (tj. w celu, o którym mowa w art. 6 ust. 1 lit. e RODO,
6. wniesienia skargi do organu nadzorczego (art. 77 RODO), tj. Prezesa Urzędu Ochrony Danych Osobowych, w przypadku uznania, że przetwarzanie danych osobowych narusza przepisy RODO lub inne przepisy prawa regulujące kwestię ochrony danych osobowych.

Zautomatyzowane podejmowanie decyzji

Dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Przekazywanie danych do państwa trzeciego

Nie zamierzamy przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej innej niż Unia Europejska. W przypadku konieczności przekazania Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej zapewniamy, że odbędzie się to z zachowaniem warunków określonych w art. 45 lub 46 RODO.

Kontakt z administratorem danych i Inspektorem Ochrony Danych

Jeśli mają Państwo pytania dotyczące przetwarzania przez CPPC danych osobowych, prosimy kontaktować z Inspektorami Ochrony Danych Osobowych (dalej jako IOD) w następujący sposób:

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

1. IOD MFiPR:
   1) pocztą tradycyjną kierując korespondencję na adres: ul. Wspólna 2/4, 00-926 Warszawa,
   2) elektronicznie na adres e-mail**:** **IOD@mfipr.gov.pl**,
2. IOD CPPC:
   1) pocztą tradycyjną kierując korespondencję na adres: ul. Spokojna 13A, 01-044 Warszawa,
   2) elektronicznie na adres e-mail: **bezpieczenstwo@cppc.gov.pl**.

Podstawa prawna:

1. ustawa wdrożeniowa – ustawa z 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. z 2022 r., poz. 1079),
2. RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE. L 119 z 4 maja 2016 r., s. 1-88; Dz. Urz. UE L 127 z 23 maja 2018, str. 2 oraz Dz. Urz. UE L 74 z 4 marca 2021, str. 35).

Podmiot przetwarzający:

Starostwo Powiatowe w Nowym Mieście Lubawskim, ul. Rynek 1, 13-300 Nowe Miasto Lubawskie, mail: **iod@powiat-nowomiejski.pl**.

Załączniki:

1. Formularz oferty.
2. Oświadczenie o braku powiązań z Zamawiającym i braku podstaw do wykluczenia.
3. Wykaz usług.
4. Wykaz osób przeznaczonych do realizacji zamówienia.
5. Projektowane postanowienia umowy (części 1. i 2. zamówienia).
6. Projektowane postanowienia umowy (część 3. zamówienia).

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa